

[NEWS] Citrix Metaframe XP is vulnerable to Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0015.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/02/03

To: list@securiteam.com

Date: 2 Nov 2003 19:07:58 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Citrix Metaframe XP is vulnerable to Cross Site Scripting

SUMMARY

The Citrix MetaFrame Access Suite is a product that enables users to access enterprise applications and information on demand. MetaFrame XP is vulnerable to a Cross-Site Scripting attack based on the manipulation of error messages sent to user's web browser.

DETAILS

Vulnerable systems:

- * Citrix MetaFrame XP 1.0
- * Web Interface 2.0

During a recent penetration test, IRM identified a machine running Citrix MetaFrame XP that prompted for authentication credentials. When 'random' credentials were supplied, a page was returned displaying the following error:

"ERROR: The credentials supplied were invalid. Please try again."

The text used to construct this error message formed part of the URL:

https://server/citrix/metaframexp/default/login.asp?NFuse_LogoutId=On&NFuse

Securiteam: [NEWS] Citrix Metaframe XP is vulnerable to Cross Site Scripting

MessageType=Error&NFuse_Message=Thex0020credentialsex0020suppliedx0020werex0020invalidx002ex0020x0020Pleaseex0020tryx0020againx002e

If the URL was changed to the following:

[https://server/citrix/metaframexp/default/login.asp?NFuse_LogoutId=On&NFuse_MessageType=Error&NFuse_Message=<SCRIPT>alert\("Vulnerable to XSS"\)</SCRIPT>](https://server/citrix/metaframexp/default/login.asp?NFuse_LogoutId=On&NFuse_MessageType=Error&NFuse_Message=<SCRIPT>alert("Vulnerable to XSS")</SCRIPT>)

The server processed the HTML and executed the JavaScript on the user's browser.

Citrix were contacted and immediately confirmed that this was indeed a security issue and set about producing a patch to include in the next update for the product.

Vendor & Patch Information:

Citrix were contacted on August 18th 2003 and released the update on October 2nd 2003, which can be downloaded from <<http://www.mycitrix.com>> <http://www.mycitrix.com>.

Workarounds:

IRM are not aware of any workarounds for this issue.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:advisories@irmplc.com>> IRM Advisories.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.